

跨境电商平台犯罪风险防控挑战及应对路径

吴劲昊

贵州大学法学院, 贵州 贵阳

收稿日期: 2025年3月11日; 录用日期: 2025年4月3日; 发布日期: 2025年5月7日

摘要

随着互联网技术的快速发展和全球化进程的不断深入,跨境电商平台已成为国际贸易的重要渠道。然而,伴随着跨境电商的蓬勃发展,各类犯罪风险也随之而来,对平台安全、用户权益和国家安全造成严重威胁。本文深入探讨了跨境电商平台主要犯罪特点以及犯罪趋势,在此基础上,分析了当前跨境电商平台犯罪风险防控面临的挑战,如法律规制碎片化、监管效能赤字、技术手段代差、平台承担责任法理相悖、犯罪构成要件异化等。针对上述挑战,本文提出了多维度的应对路径:完善相关法律法规体系,建立健全跨境协作机制,加强平台自身风险管理能力,运用先进技术手段提升防控水平。通过多方位、多层次的防控措施,旨在构建一个安全、可信、高效的跨境电商生态系统,促进跨境电商行业的健康可持续发展。

关键词

跨境电商平台, 犯罪风险, 风险防控, 技术创新

Challenges and Response Paths for Crime Risk Prevention and Control on Cross-Border E-Commerce Platforms

Jinhao Wu

School of Law, Guizhou University, Guiyang Guizhou

Received: Mar. 11th, 2025; accepted: Apr. 3rd, 2025; published: May 7th, 2025

Abstract

With the rapid development of Internet technology and the deepening process of globalization, cross-border e-commerce platforms have become an important channel for international trade. However, with the booming development of cross-border e-commerce, various criminal risks have

also emerged, posing a serious threat to platform security, user rights, and national security. This article delves into the main criminal characteristics and trends of cross-border e-commerce platforms. Based on this, it analyzes the challenges faced by current cross-border e-commerce platform crime risk prevention and control, such as fragmented legal regulations, regulatory efficiency deficits, technological differences, conflicting legal responsibilities of platforms, and alienation of criminal elements. In response to the above challenges, this article proposes a multidimensional response path: improving the relevant legal and regulatory system, establishing a sound cross-border cooperation mechanism, strengthening the platform's own risk management capabilities, and using advanced technological means to enhance the level of prevention and control. Through multi-faceted and multi-level prevention and control measures, the aim is to build a safe, trustworthy, and efficient cross-border e-commerce ecosystem, and promote the healthy and sustainable development of the cross-border e-commerce industry.

Keywords

Cross Border E-Commerce Platform, Criminal Risk, Risk Prevention and Control, Technological Innovation

Copyright © 2025 by author(s) and Hans Publishers Inc.

This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).

<http://creativecommons.org/licenses/by/4.0/>



Open Access

1. 引言

近年来跨境电商蓬勃发展，为全球贸易注入新活力。然而，由于跨境电商平台的匿名性、虚拟化、跨境性等特征导致相关部门难以实现有效监管，从而为违法犯罪活动提供了温床，信息泄露、走私、侵犯知识产权、逃税等犯罪风险日益凸显。传统监管手段在应对跨境电商平台犯罪时面临诸多挑战，如法律适用冲突、管辖权争议、证据收集困难、平台责任界定不清等。因此，如何有效防控跨境电商平台犯罪风险，成为学术研究和实践亟待解决的课题。本文将从法律规制、平台责任、国际合作等角度，探讨跨境电商平台犯罪风险防控的挑战及应对路径。

2. 现行态势：跨境电商平台犯罪风险防控现状分析

2.1. 跨境电商平台犯罪的特点

跨境电商平台的全球化、数字化与去中心化特质，从根本上重构了犯罪行为的生成逻辑与表现形式，致使相关犯罪活动呈现出跨境性、虚拟性、技术驱动性及犯罪链条专业化等规范层面的系统性风险。其核心特征体现为：在空间维度上，犯罪行为因平台的无国界属性天然嵌入多重法域，犯罪主体、实行行为与危害结果常分散于不同司法辖区，致使法律适用面临规范冲突与管辖权竞合的双重困境，典型如商品生产、跨境物流与支付结算等环节的跨国分工协作，客观上形成规避单一法域监管的隐蔽性架构；在技术维度上，交易主体通过虚拟身份认证机制实现的匿名化交互，叠加数字商品(如软件授权密钥)与虚拟服务(如在线课程)的非实体化流转特性，严重削弱了传统监管手段对洗钱、诈骗等犯罪行为的追溯能力；在组织维度上，犯罪活动已演化为高度专业化的产业链形态，涵盖技术支持(如爬虫程序开发)、资金通道(加密货币混币服务)与物流配套(虚假报关单据制作)等环节的精密分工，形成兼具技术赋能与风险隔离功能的“灰黑产”协同网络。

跨境电商平台犯罪的技术驱动性特征在数字时代呈现出鲜明的规范挑战，其核心体现为犯罪手段与

前沿技术的高度耦合性。犯罪分子通过技术中立外衣下的工具野蛮扩张,将深度学习、数据爬取等技术嵌入犯罪实行行为,通过利用深度伪造(Deepfakes)技术伪造商品展示信息与通过“爬虫”技术窃取用户数据。犯罪分子通过深度伪造(Deepfakes)技术系统性解构商品信息的真实性边界,该技术依托生成对抗网络(Generative Adversarial Networks)的算法架构,将低分辨率面部图像经特征提取与三维建模后生成具有欺骗性的视听内容,实质上架空了传统法秩序对“物证真实性”的推定基础。这项技术实现了内容呈现从全然真实到具有欺骗性的转变[1]。与此同时,自动化数据爬取行为的技术本质与刑事违法性判定呈现规范张力,爬虫程序基于预设规则遍历网络节点抓取数据的过程,在技术层面符合《刑法》第 285 条非法获取计算机信息系统数据罪中“侵入或采用其他技术手段”的客观要件,但当其突破平台 Robots 协议或实施流量劫持时,可能触发第 285 条第 2 款非法控制计算机信息系统罪的适用[2]。技术中立表象下,跨境电商平台此类行为实质形成技术滥用与法律规避的双重效应。

2.2. 跨境电商平台犯罪的趋势

跨境电商犯罪形态呈现系统性演进趋势,其核心机理表现为技术赋权、行为异化与规制失范的三角张力结构。从犯罪学视角分析,该领域正经历三个维度的范式突破:其一,技术迭代重构犯罪构成要件,区块链、生成式人工智能等新兴技术催生新型犯罪模式,形成技术黑箱效应;其二,犯罪网络呈现跨区域协同特征,支付结算、物流仓储、数据流转等环节形成犯罪生态链;其三,规范体系面临代际脱节困境,传统属地管辖原则与平台中立责任理论在应对分布式犯罪结构时显现制度性疏漏。值得注意的是,技术渗透指数与犯罪隐蔽程度呈显著正相关,新型数字工具已深度嵌入犯罪全流程,这对刑事证明标准与侦查技术构成实质性挑战。

技术工具的应用比例呈现爆发式增长,加密货币支付、区块链数据隐匿及深度伪造技术的使用率极速增长,且技术犯罪隐蔽性较传统手段显著提升,直接导致《刑法》第 285 条非法获取计算机信息系统数据罪等条款的构成要件面临“技术性规避”困境。尽管区块链存证与 AI 分析等技术辅助手段将证据跨境调取成功率提升但犯罪收益追缴率仍停滞于较低层面,暴露出《联合国反腐败公约》资产追回机制在应对加密货币混币器、去中心化金融工具时的制度性失灵。更深层次的矛盾在于,算法推荐系统的技术异化衍生出“犯罪扩散加速器”效应,平台算法对违规商品流量的非中立分配行为,已实质性突破《电子商务法》第 42 条技术中立原则的免责边界,亟待通过刑法教义学对“算法共谋”行为构建实质归责模型。

需特别指出的是,上述趋势分析受限于犯罪“暗数”效应与技术迭代速度,实际犯罪规模与新型风险(如生成式 AI 诈骗)可能远超已有数据范畴。该态势倒逼法学研究从被动解释转向主动建构,通过技术要素的规范类型化、平台责任的刑法实质化(增设算法治理义务条款)及国际司法协作的规则创新,方能实现数字时代犯罪防控范式的系统性重构。

3. 成因分析:跨境电商平台犯罪风险防控面临的挑战

3.1. 法律规制体系的碎片化

3.1.1. 法律适用的多元冲突

跨境交易行为同时受制于商品/服务提供地、消费地、平台注册地等多法域法律规范,各国在数据主权、消费者保护、知识产权等领域的立法差异形成“制度洼地”。欧盟《通用数据保护条例》(GDPR)依据其原则,无论数据处理行为是否发生在欧盟境内,只要涉及向欧盟居民提供商品/服务或监控其行为,均受 GDPR 约束。但在发展中国家实践中,印度《个人数据保护法》(PDPB)、印度尼西亚《数据保护法》等要求特定类型数据(如公民个人信息、金融数据)必须存储于境内服务器,并限制向未签订数据协定的国

家传输[3]。例如,越南《网络安全法》第26条强制要求境内互联网企业将用户数据本地化存储。总而言之, GDPR 要求数据自由流动至符合其标准的国家,而发展中国家通过数据本地化立法限制数据出境,形成“合规互斥”。欧盟《通用数据保护条例》(GDPR)与部分发展中国家数据流通规则的冲突,客观上为数据滥用犯罪提供制度套利空间。

3.1.2. 管辖权规则的竞合困境

由于跨境电商平台的全球性特征,其交易活动可能同时受多个国家的管辖权规则影响,这导致在实际操作中出现管辖权规则的竞合现象。即同一案件可能由多个国家或地区的法院同时主张管辖权,从而引发法律冲突和不确定性。传统属地管辖原则难以应对“行为要素跨国离散化”特征。商品展示(服务器所在地)、支付结算(金融监管地)、物流交付(海关管辖地)等环节分属不同法域,导致刑事管辖权积极冲突与消极冲突并存[4]。国际法上的“实际控制原则”与“效果原则”在司法实践中常引发主权摩擦。

3.2. 平台责任承担的法理悖论

3.2.1. 技术中立的规则局限

技术中立原则是指政府或立法机构对于各种有关电子商务的技术、软件、媒体等采取中立的态度,由实际从事电子商务者和信息服务中介商自己根据技术发展选择采取新的或与国际社会接轨的技术。政府应当不偏不倚,鼓励新技术的采用和推广。技术中立的规则局限主要体现在法律评价与技术本质之间的脱节。技术中立性强调工具本身无善恶之分,但法律需对具体行为进行价值判断,导致技术应用的法律边界模糊。现有法律规则往往难以精准区分技术的中立属性与行为的违法性,使得实践中出现过度规制或执法空白。跨境电商平台抓住执法空白的漏洞,通过算法推荐客观上助长犯罪行为发生,而后以技术中立抗辩规避刑事风险,这一做法突破了技术中立的原则。跨境电商平台常以《电子商务法》第42条技术中立抗辩规避审查义务,但其实质帮助行为正逐步突破形式中立边界。当平台算法推荐客观上促成假冒伪劣商品扩散时,其注意义务的边界亟待刑法教义学重构,技术中立原则不应被异化为平台规避刑事风险的工具性屏障。技术中立性作为一项旨在区分技术本身与其应用行为的理论框架,其核心在于强调技术的工具属性,而非为平台主体提供绝对化的免责依据。

3.2.2. 合规激励机制的失衡

现行法律对平台的事前预防责任(如商户资质审核)与事后处置责任(如数据留存)规定呈现“重行政轻刑事”倾向[5]。在司法实践中,对于平台预防以及事后处置不当的行为常常以行政手段进行规制。由于执法机关对跨境电商平台的宽容性与自由性导致跨境电商平台变本加厉反复横跳在违法犯罪边缘。平台在“合规成本-收益”博弈中易形成“象征性治理”,对于其预防责任与事后处置责任全然不顾。

3.3. 国际刑事司法协作的效能赤字

一方面,不同国家之间的法律体系存在差异,导致在司法协助过程中产生法律冲突和解释上的困难。某些国家可能出于司法主权考虑,对特定类型的司法协助请求持谨慎态度,因此程序进展缓慢。各国在加入《海牙取证公约》时,对公约中的某些条款提出保留。这些保留条款限制了公约在某些方面的适用,增加了司法协助的复杂性和耗时。《海牙取证公约》框架下的司法协助程序耗时漫长,与跨境电商犯罪证据(如电子交易日志、加密通信记录)的瞬时湮灭性形成尖锐矛盾[6]。部分国家数据本地化立法进一步加剧刑事司法取证困境。以上种种无一不彰显证据跨境调取存在制度壁垒。

另一方面,随着虚拟货币、离岸金融账户等新型洗钱工具的出现,全球腐败与犯罪资产追缴体系正面临前所未有的挑战。传统以《联合国反腐败公约》为核心的资产追回机制,本质上依赖于对银行账户、

不动产等“有形资产”的追踪和冻结，其逻辑建立在“中心化监管”基础上——即各国金融机构需配合披露资金流向，执法机关通过冻结令即可截断资产转移链条。然而，虚拟货币依托区块链技术的匿名性与去中心化特征，彻底颠覆了这一模式。犯罪分子只需几行代码，便可将赃款瞬间拆解为无数加密代币，通过混币器、跨链桥等技术手段在全球匿名钱包间跳跃流转，如同将一杯水倒入大海后再用针尖舀出，传统执法中的“账户冻结”完全失去抓手。由于虚拟货币、离岸账户等新型洗钱路径导致《联合国反腐败公约》资产追回机制失灵，犯罪所得跨境转移呈现“去中心化”特征，传统冻结扣押措施面临现实性失灵，犯罪收益追缴的实践梗阻巨大。

3.4. 技术赋能与法律滞后的结构性矛盾

智能算法推荐、深度伪造(Deepfake)商品展示等技术的应用，使得“恶意合规规避”行为具有更强的隐蔽性与扩散力。现有法律对“算法共谋”“数据投毒”等新型犯罪预备行为缺乏类型化规制，形成“技术代差”风险。智能算法推荐系统，通过分析用户的个性化需求和行为模式，能够精准推送内容或商品，极大地提升了用户体验和商业效率。犯罪分子利用智能算法，进行隐蔽的恶意合规规避，实现不公平的市场竞争。由于算法的黑箱特性，这些违规行为往往难以被及时发现和查证，从而增加了执法的难度[7]。深度伪造(Deepfake)技术的商品展示应用，更是将虚假信息的传播提升到了一个全新的高度。通过高度逼真的图像和视频合成技术，不法商家可以轻易制作虚假的商品展示视频，误导消费者，损害公平竞争的市场环境。

现有法律体系在面对这些新型犯罪预备行为时，显得力不从心。由于算法共谋的隐蔽性和复杂性，现有法律对其缺乏类型化规制，导致执法机构在打击此类行为时面临重重困难。这种技术赋能与法律滞后的结构性矛盾，不仅加剧了市场竞争的不公平性，也增加了执法和司法的难度。随着技术的不断发展，这种矛盾可能会进一步加剧，形成所谓的“技术代差”风险，即由于法律体系的更新速度无法跟上技术发展的步伐，导致法律体系在规制新型犯罪行为时存在明显的滞后性和不足[8]。

4. 路径选择：跨境电商平台犯罪风险防控的应对路径

4.1. 法律规制体系碎片化的破解路径

4.1.1. 构建阶梯式法律适用规则

制定跨境电商刑事司法协助专门公约，在联合国国际贸易法委员会(UNCITRAL)框架下制定《跨境电商刑事司法协助公约》，明确洗钱、走私等核心犯罪行为的“最低限度规则”，确立各国刑事立法的趋同义务[9]。在跨境交易场景中引入《罗马条例 I》中的“最密切联系原则”，建立以“消费者惯常居所地法”为主、兼顾“平台主要营业地法”的冲突规范体系，通过《海牙国际私法会议》推动形成区域性跨境电商法律适用示范条款。针对数据主权冲突，本质是数字时代“权利本位”与“发展本位”治理范式的碰撞。应当推动欧盟与发展中国家签署“等效性+”协议，允许部分领域(如电商交易数据)适用简化合规程序。唯有通过规则互操作性设计，方能实现数据保护与流通价值的动态平衡。

4.1.2. 制定实质损害结果发生地管辖的规则

破解跨境电商犯罪治理困局需重构管辖权理论模型。传统属地管辖原则在应对“生产环节在 A 国、服务器架设在 B 国、消费者遍布 C 至 E 国”的犯罪要素离散化格局时，已显现结构性失灵，机械适用“犯罪行为地”或“结果发生地”标准将引发数十个司法辖区的管辖权混战。对此，可构建“实质损害结果”规则：以消费者财产损失、公共健康危害等可量化的实害结果集中爆发地作为管辖权优先连接点。例如，某跨境电商业者销售含禁用成分的减肥药，当中国消费者因药物副作用集中就医时，即便服务器

位于开曼群岛、支付系统注册于新加坡，仍应由中国法院优先行使管辖权。同时，为消解各国司法主权敏感性问题，可在国际刑事法院框架下创设常设性跨境电商犯罪专家委员会。该委员会可由多名具备刑事司法经验的国际法官、电子取证技术专家及电商平台法务代表组成，建立咨询：当两国对管辖权归属产生争议时，首先启动外交层面的紧急磋商；若规定时间内未达成共识，则自动触发专家委员会介入程序。委员会根据“消费者权益受损比例”“证据集中度”“执法可行性”三维度评估体系出具咨询意见。以某跨境代购假药案为例，当售假商家在德国注册、仓储设于波兰、主要受害者在法国时，专家委员会可通过分析销售数据热力图(显示 75% 订单流向法国)、服务器日志留存情况(法国消费者聊天记录完整留存)等要素，建议由法国司法机关主导调查，同时要求德国配合冻结涉案账户。这种“动态管辖权分配”机制既突破“全有或全无”的传统管辖思维，又通过国际组织的中立协调避免主权对抗。

4.2. 平台责任结构的法理悖论破解

4.2.1. 明确算法推荐行为的刑事可归责性

通过刑法解释将平台算法推荐行为纳入《刑法》第 287 条之二“帮助信息网络犯罪活动罪”的规制范围：当算法系统主动推送明显违法商品(如假冒奢侈品)时，可认定平台具有“明知或应知”的主观要件。引入德国刑法中的“组织责任理论”，要求平台对入驻商家建立“风险分级管理体系”，未履行分类监管义务导致犯罪发生的，承担过失不作为责任。平台必须承担预防责任以及事后处置责任，事前需对入驻平台的机构与用户进行资质审查，事后需做到完整保留机构与用户数据以便审查。平台负有组织责任义务，在不限平台良性发展的前提下进行合理规划，倒逼平台参与犯罪风险防控之中。

4.2.2. 合规激励机制的重塑

建立“合规量刑激励机制”参照美国《联邦量刑指南》中的合规计划评价标准，将平台合规体系建设情况(如 AI 风控系统覆盖率、商户审核响应速度)作为量刑从宽情节，通过《刑法》第 37 条之一“从业禁止”条款反向强化合规动力。在《电子商务法》中增设“合规成本补偿机制”，允许平台将犯罪防控支出(如区块链溯源技术投入)纳入税前抵扣范围。通过以上措施的设立，激励跨境电商平台进行自我审查。平台未做到忠实勤勉义务将会受到行政责任与刑事责任的追究，不仅面临停业整顿的行政处罚也会面临刑事处罚。避免平台不作为甚至乱作为的发生，让其在“合规成本 - 收益”模型中实现合规成本大于违法收益。

4.3. 建立云协查机制与虚拟货币流向检测链

在数字经济全球化背景下，跨国犯罪呈现“链式分布、瞬时湮灭”的技术特征，因此突破《海牙取证公约》的取证困局需要构建“阶梯响应”机制：对于普通电子证据，仍适用公约规定的司法协助程序；对于具有易失性特征的云端数据(如即时通讯软件缓存、远程服务器日志)，可依据《布达佩斯公约》第 32 条 b 款启动紧急协查程序，由数据所在国节点在 48 小时内完成司法审查并反馈；针对涉及恐怖融资、人口贩卖等重大犯罪的关键证据，可通过平台内置功能进行非接触式取证，原始数据仍受主权管辖但镜像副本具备法定证明力。该机制已在欧盟“麒麟计划”反恐行动中完成实战验证。授权执法部门在紧急情况下跨境提取易灭失电子证据，通过云协查机制避免犯罪证据的瞬时性湮灭从而更好的打击犯罪^[10]。同时，由国际反洗钱组织(FATF)主导建立跨境加密货币交易追踪联盟链，要求各国交易所接入节点并共享可疑交易地址标签库。修订《联合国反腐败公约》第 54 条，将“推定违法所得”规则适用于利用混币器处理的加密货币资产，破解举证难题。对于虚拟货币流向检测直接关系到违法所得的追缴问题，直接影响到社会经济秩序的发展。正是因为犯罪所得难以追缴才会导致此类犯罪的频繁发生，正所谓“重赏之下必有勇夫”。通过构建虚拟货币流向检测链，彻底粉碎犯罪分子“人进去，钱还在”的幻想，不仅人要进去

违法所得也必将追回。

4.4. 确立算法备案与审查制度

在《网络安全法》中增设平台算法备案义务,要求跨境电商平台向监管部门报备商品推荐算法逻辑,对可能诱发犯罪的算法模型(如“假冒商品优先推荐模型”)实施强制下架。平台的算法模型必须经过专业部门的检测方可投入使用,并且一旦发现检测模型与实际运用模型不一致,将依法追究平台的刑事责任。平台将不能以技术中立规避刑事犯罪风险,必须在相关部门的监管下进行技术创新。同时,应当借鉴欧盟《数字服务法》(DSA)第27条,赋予司法机关“算法审计权”,可委托第三方技术机构对平台算法进行逆向工程检测。对于不符合要求的平台算法必须一律追究其责任。有关部门应当不定时进行算法审查,将相关数据统计公之于众,让用户避免去更高风险的跨境电商平台进行活动。通过事前预防以及事后检查,将规范跨境电商平台算法行为。

5. 结语

跨境电商平台犯罪治理需实现从“被动回应”向“主动塑造”的范式转换。通过法规创新、平台责任刑法化改造、国际司法协作机制升级与技术治理工具嵌入,构建“法律-技术-制度”三位一体的风险防控体系。这既需要法学理论对数字时代犯罪形态的深刻回应,更依赖国际社会在规则互认、数据共享与技术标准协同上的实质性突破。

参考文献

- [1] 郭子淳,李萌,孟宪宁. AI 涌现式生成对视听创作的挑战:面向未来视听产业的几点思考[J]. 中国电视, 2024(12): 31-37.
- [2] 高永明,马光远. 网络爬虫的规制逻辑: 行政监管前置的路径提倡[J]. 吉林大学社会科学学报, 2024, 64(3): 73-86+236.
- [3] 柏婉丹. 欧盟数据跨境流动规则对我国企业的启示[J]. 中阿科技论坛(中英文), 2025(2): 143-147.
- [4] 秦多佳. 跨境电子商务平台在线纠纷解决管辖权问题研究[D]: [硕士学位论文]. 上海: 华东政法大学, 2023.
- [5] 苏琳琳. 跨境电商企业推单行为研究[J]. 中阿科技论坛(中英文), 2023(9): 148-152.
- [6] 钱颜. 国内首例跨境电商不正当竞争案二审维持原判[N]. 中国贸易报, 2024-10-17(006).
- [7] 冯培睿,陈希,张蕊馨. 跨境社交网络犯罪治理下的国际网络安全维护手段合作问题[J]. 中阿科技论坛(中英文), 2024(7): 167-172.
- [8] 张月珊. RCEP 背景下跨境电商的法律保障及风险防范[J]. 法制博览, 2023(20): 94-96.
- [9] 张晓君. 论数据管辖权的冲突与协调[J]. 政法论丛, 2025(1): 95-109.
- [10] 黎晓露. 跨境数据取证的国际博弈与中国方案[J]. 证据科学, 2023, 31(6): 693-705.